OUTLINE OF RESEARCH WORK ENTITLED

Study of Weight Distribution Properties of Linear Codes

Submitted to

Swami Ramanand Teerth Marathwada University

Nanded-431606, Maharashtra State, India

For Registration of (Ph.D.) Doctor of Philosophy in Mathematics

Research Student

Ms. Shinde Pranita Prabhu

Under the Guidance of

Dr. Arunkumar R. Patil

Department of Mathematics,
SGGS Institute of Engineering and Technology,
Swami Ramanand Teerth Marathwada University,
Nanded-431606, Maharashtra, India.

April 2022

1 Introduction

Coding theory lies naturally at the intersection of a large number of disciplines in pure and applied mathematics i.e. algebra and number theory, probability theory and statistics, communiction theory, discrete mathematics and combinatorics. The problem of determination of higher weights of linear codes has attracted many researchers from mathmatics as well as engineering. The set of all possible weights of a linear code is called weight distribution of a code. Various structural properties of a code can be explored through the determination of its weight distribution. The concept of higher weights of linear codes was first introduced by Victor Wei in 1991 [2] , to study the classical problem of "wire tap-channel of type II" from cryptography. Soon after Feng, Tzeng and Wei studied the generalized Hamming weights for BCH and other cyclic codes [3]. I am motivated to study the higher weights of linear codes. More specifically, I am interested in the study of higher weights of special cyclic codes such as quasi cyclic codes, nega cyclic codes, consta cyclic codes. I would like to develop algorithms to determine the weight distribution of these code and also study a problem of determining (usual) spectrum of such codes.

2 Review of Literature and development in the subject

The subject coding theory arose due to practicle problem in reliable communication of digitally encoded information. Claude Shannon's 1948 paper , *"A Mathematical Theory of Communication"* gave birth to coding theory. A mathematical problem originating in electrial engineering is the recovery of a signal which is transmitted over a noisy medium where chances to occur error. The goal of coding theory are to develop systems and methods that allow to detect/correct errors caused when message is sent through such noisy channels. The message is a block of symbols from finite alphabet, say $\{0, 1\}$. These alphabets have great algebraic structure. Many areas of mathematics are used in coding theory and we focus on the interplay between algebra and coding theory. Let $\mathbb{F}_q^n$ denote the vector space of all n-tuple over a finite field $\mathbb{F}_q$. An (n, k) linear code

C is a $k-$dimensional subspace of the vector space $\mathbb{F}_q^n$ with $M = q^k$ elements, $C = \{c_1, c_2, ..., c_M\}$ where $c_i = (c_{i0}, c_{i1}, ..., c_{i(n-1)})$ are called the codewords of C. The linear property assures that if $c_i, c_j \in C$ and $f \in \mathbb{F}$, then $fc_i + c_j \in C$. A generator matrix G for an (n, k) code C is a $k \times n$ matrix whose rows form a basis for C. The generator matrix in the form $G = [I_k : A]$. A parity check matrix H for an (n, k) code C is an $(n-k) \times n$ matrix, whose rows are linearly independent such that $C = \{x \in \mathbb{F}_q^n | Hx^T = 0\}$ where x^T denotes the transpose of x. Each Hx^T is called a parity check matrix. Parity check matrix is itself a generator for an $(n, n-k)$ code called the dual code denoted $C^\perp$. The parity check matrix in the form $H = \{A^T : I_{n-k}\}$. Number of position between two code x and y, where the codeword have different symbols is called Hamming distance and it is denoted by $d(x, y)$. The number of nonzero entry in any code is called Hamming weight of the code and denoted by $w(x) = d(x, 0)$. The minimum distance of code C, denoted d is the smallest distance between distinct codewords of the code. Since $d(x, y) = w(x - y)$, the minimum distance of a code C is also equal to the smallest weight of non-zero codeword. These parameters n, k, d determine how best is a given linear code. That means we can detect k or fewer error iff $d \geq k + 1$ and also we can correct k or fewer error iff $d \geq 2k + 1$. Let C be an $[n, k]$ code with $D \subset C$ a subcode. The support of D, denoted $\chi(D)$, is the set of not-always-zero bit positions of D, i.e., $\chi(D) = \{i : \exists(x_1, x_2, ..., x_n \in D, x_i \neq 0)\}$. Let D be a one-dimensional subcode of C. The size of the support of D equals the Hamming weight of the non-zero codeword in D. Hence, the minimum distance of C is the minimum of $|\chi(D)|$ as D ranges over all one-dimensional subcode of C.Wei generalized this difination. The r^{th} generalized Hamming weight of C, denoted by $d_r(C)$, is the smallest support of an $r-$ dimensional subcode of C. That is, $d_r = min\{|\chi(D)| : D$ is a subcode of C with rank $r\}$. We can also assemble all generalized Hamming weights of a code to form the weight hierarchy. The weight distribution of a linear code C is defined to be the set of integers $\{d_r(C) : 1 \leq r \leq k\}$. Weight distribution of a linear code C is also called weight heirachy of C. For an $[n, k]$ code C with $k > 0$, we have $1 \leq d_1(C) < d_2(C) < ... < d_k(C) \leq n$. For an $[n, k]$ code C, $d_r(C) \leq n - k + r$ which is Generalized Singleton Bound. When $r = 1$, this is the Singleton bound. The relation between generalized weights of C and the generalized weights of the dual code $C^\perp$ is

given by the following relation;

$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, ..., n\}$ / $\{n = 1 - d_r(C^{\perp}) : 1 \leq r \leq n - k\}$. A linear code C of length n over finite field $\mathbb{F}_q$ is called a cyclic code if for every codeword $c \in C$ the codeword obtained by a cyclic shift is also a codeword in C. That is $c = (c_0, c_1, ..., c_{n-1}) \in C \Rightarrow c' = (c_{n-1}, c_0, ..., c_{n-2}) \in C$. Every codeword $c \in C$ can be represented as polynomial of degree at most $n-1$. There are various cyclic codes such as BCH codes, Reed Solomon codes, which have been used due to their error detection and correction capabilities [12, 15]. This property can naturally be connected to quasi cyclic code. That is Quasi cyclic codes are generalisation of cyclic code. A linear block code C of length $n = ml$ over a finite field $\mathbb{F}_q$is called a quasi cyclic code of index l if for every codeword $c \in C$ there exists a number l cyclic shifts is also codeword in c i.e. $c = (c_0, c_1, ..., c_{n-1}) \in C \Rightarrow c' = (c_{n-l}, \ldots, c_0, \ldots, c_{n-l-1}) \in C$. Cyclic codes are quasi cyclic codes with $l = 1$. The ideal generated by irreducible factors of $x^n - 1$ leads to the class of cyclic codes. But, in general for a nonzero constant $\lambda \neq 1$, the factorization of $x^n - \lambda$ leads a another very beautiful class of cyclic codes called constacyclic codes. These codes have become interest of research recently. Various researchers have studied in the minimum Hamming weights of negacyclic and cyclic codes of length p^s over finite field of characteristic p are determined. Recently, Alessio Meneghetti, Marco Pellegrini, Massimiliano Sala, C.Golubitsky [1], T Klove have developed in weight distribution properties of linear code.

3 Aim and Objective of Research

The main objective of my research during Ph.D. is to work on weight distribution properties of linear code.

(i) We will investigate and expand some properties of weight distribution of linear codes from the family of cyclic codes such as quasi cyclic, Nega cyclic, Consta cyclic code.

(ii) We will also interested to investigate the usual spectrum of this family linear codes.

4 Methodology to be adopted

My area of research is theoretical in nature. Mostly, I will be referring the text books and research papers of various researchers who have developed this area of research.The procedures or techniques used to identify, select,process and analyse information about a topic. I would also like to consult with my thesis supervisor time to time to discuss the doubts regarding to this topic. I would also like to participate in the schools, seminars,conferences, workshops in my area of research, which will help me to strengthen my knowledge in my field of research.

5 Importance of study

The area of my research is very interesting and highly applicable in coding theory. Coding theory has its origins in the engineering problem of effective electronic communication where the alphabet is generally the binary field. Since its inception, it has grown as a branch of mathematics.The determination of the weight distribution of linear codes has been a fascinating problem since the very beginning of coding theory.Many problems in coding theory require efficient computing of weight distribution of given linear code.Some sufficient conditions for a linear code to be good or proper for error detection are expressed in terms of the weights distribution.This proposal will presents a broad view of the subject and relates major results on weight distribution.

6 Proposed Work Plan

Following is the Year-wise plan of work and target to be achieved during my research period:

Year 1:

Course work and reading : I will complete the course work and other academic formalities declared by SRTMU Nanded in the first semester. Then after, I would like to read the following text books to develop necessary background for my research:

(i) R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, (1994).

(ii) F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

Year 2:

I would like to read the research papers, text books, and would like to complete research related literature survey and decide the problem for my PhD thesis in consultation with my thesis supervisor. I would also like to participate in various national and international workshops, schools and conferences to get the broader view and to develop academic relations with other reserachers who are working in my field. **Year 3**: I will focus on my research problem and would like to learn various techniques and methods by the other researchers on my area of research.

Year 4: I will try to solve my thesis problem and try to have my publications related to my work.

Year 5: I will try to write my thesis and submit to university for the award of PhD.

References

[1] Chaos Golubitsky, Weight distribution of linear Error correcting codes.

[2] Victor K.Wei, Generalized Hamming Weights for Linear Codes, Transactions on Informaton Theory, Vol. 37, NO. $5, 1412 - 1413$, September, 1991.

[3] G.L. Feig, K.K. Tzeng and V.K. Wei, On the Generalized Hamming Weights of several classes of cyclic codes, Transactions on Information Theory, Vol.38, NO. 3, 1125 -1126, May, 1992.

[4] F.J.Macwilliams and N.J.A. Sloane, The Theory of Error- Correcting Codes , North-Hollant Mathematical Library, Vol.16, Nineth Impression 1996.

[5] C. Shannon, A mathematical theory of communication. Bell Syst. Techn. J. 27 (1948).

[6] S.T. Dougherty, J. Kim, P. Sole, Open problems in coding theory, Contemp. Math. 634, 79-99 (2015).

[7] S.T. Dougherty, A. Kaya, E. Salturk, Cyclic codes over local frobenius rings of order 16. Adv. Math. Comm. 11(1), 99-114 (2017).

[8] M. Shi, A. Alahmadi, and P. Sole,Codes and Rings: Theory and Practice, Academic Press (2017).

[9] K. Guenda, New MDS self-dual codes over finite fields, Des. Codes Cryptogr., 62, 31-42 (2012).

[10] B. Yildiz and S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Cryptogr., 58, 221-234 (2011).

[11] S. Zhu and L. Wang, A class of constacyclic codes over $\mathbb{F}_p + u\mathbb{F}_p$ and its Gray image, Discrete Mathematics, 311, 2677-2682 (2011).

[12] R. T. Chien, Cyclic Decoding Procedure for the Bose-Chaudhuri-Hocquenghem Codes, EEE Trans. on Inf. Th., vol. 10, p. 357-363, 1964.

[13] T. Abualrub and I. Siap, Constacyclic codes over F2 + uF2, J. Franklin Inst., 346, 520–529, 2009

[14] C. T. Ryan, *Projective codes based on Grassmann varieties* , Congr. Numer. 57, 273-279, 1987

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error Correcting Codes*, North Holland, Amsterdam, 1977.

[16] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometric Codes*, Kluwer, Amsterdam, 1991.

[17] S. R. Ghorpade and G. Lachaud, *Hyperplane sections of Grassmannians and the number of MDS linear codes*, Finite Fields Appl. vol. 7, 468-506, 2001.

[18] S. R. Ghorpade, A. R. Patil, H. K. Pillai, *Decomposable subspaces, linear Sections of Grassmann varieties, and higher weights of Grassmann codes*, Finite Fields Appl.15, 54-68, 2009.

Ms. Shinde Pranita Prabhu
Research Student

Dr. Arunkumar R. Patil
Research Guide